PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
	)
Jagger et al.	) Art Unit: 2143
	)
Application No.: 10/072,708	) Examiner: Bilgrami, Asghar H.
	)
Filed: 02/05/2002	) Atty. Docket No.:
	) NAIIP314/01.166.01
For: SPAM REPORT GENERATION SYSTEM AND METHOD	)
	) Date: 09/04/2007
	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 07/02/2007.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue # 1:

The Examiner has rejected Claims 1-8, and 10-31 under 35 U.S.C. 103(a) as being unpatentable over Aronson et al. (U.S. Patent No. 6,654,787 B1), in view of Leeds (U.S. Patent No. 6,393,465 B2).

Group #1: Claims 1, 3, 7-8, 13-15, 17, and 27-28

With respect to the independent claims, the Examiner has relied on Col. 4, lines 51-56; Col. 5, lines 50-67; and the Abstract in Aronson along with Col. 3, lines 54-67; and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "identifying an authority hosting the network address" (see the same or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that the excerpts from Leeds relied on by the Examiner only relate to a host computer associated with a sender of an electronic mail message (see Abstract and Col. 4, lines 66-67, specifically). In addition, Leeds discloses that "if a message has purportedly been relayed through a machine named mail.frommowhere.com and the mail handling system has determined that such a machine does not actually exist, the confidence rating for the message should be increased." Clearly, determining a host computer/host name of a sender of e-mail or relay, as in Leeds, does not meet appellant's specific claim language, namely an "authority hosting the **network** address" (emphasis added), as claimed by appellant.

Further, appellant respectfully asserts that the excerpts from Aronson relied upon by the Examiner merely disclose that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)" (emphasis added). Clearly, filtering e-mail based on IP source frequency and feature extraction & analysis fails to even suggest "identifying an authority hosting the **network** address" (emphasis added), as claimed by appellant.

In addition, the Examiner argued that "Ar[o]nson disclosed that the source header data from an incoming e-mail address (aardvark@aol.com) is analyzed by the spam probes." Further, the Examiner argued that '[t]he source header data includes the ISP (in this case "aol") hosting the spammer's network address (see col.4, lines 45-67).' Appellant disagrees and respectfully asserts that the excerpt from Aronson simply discloses that "[a] spam probe is an e-mail address selected to make its way onto as many spam mailing lists as possible." Aronson continues, teaching that "[i]t is also selected to appear high up on spammers' lists in order to receive spam mailings early in the mailing process" using an e-mail address such as "aardvark@aol.com." Clearly, the mere disclosure of using an e-mail address in a spam probe, as in Aronson, completely fails to even suggest "identifying an authority hosting the **network** address" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner asserts that 'it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. email address) can in fact be the Internet service provider (ISP)' and that "it is not possible to send e-mail or electronic mail without the presence of an Internet Service Provider." The Examiner goes on to allege that in 'a SPAM mail coming from, Spammer@aol.com... "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.'

In addition, the Examiner states that "Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent mails is SPAM mail or not." The Examiner relies on Col. 3, lines 57-67; Col. 4, lines 65-67; and Col. 5, lines 13-33 from Leeds and asserts that "Leeds clearly discloses identifying the hosting authority that is hosting the network address." Finally, the Examiner states that 'appellant in his own specification on page 12 lines 9-14 has described the same "WHOIS" method to identify the ISP (hosting authority) associated with the network address.'

Appellant respectfully disagrees and notes that the above reference excerpts relied on by the Examiner merely teach that "[t]he sender's origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent" (Col. 3, lines 59-61 – emphasis added). In addition, the excerpts teach that 48941493@notarealaddress.com is

broken down into a user id (48941493) and a host name (notarealaddress.com) (Col. 4, lines 65-67 – emphasis added). Further still, the excerpts teach that '[s]ince junk e-mails often come from either non-existent users or non-existent sites or both, a first level check is to determine if the alleged sender[s] identified by the "From:" or "Reply-To:" fields are valid' and that '[t]his first level check corresponds to issuing a verification request and can be in many forms, including… using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (Col. 5, lines 16-25 – emphasis added).

However, merely extracting sender origination information, such as a host name, from an e-mail message header, and using a UNIX "whois" command to determine if the host actually exists, as in Leeds, does not teach actually "identifying an authority hosting the **network** address" (emphasis added), as claimed by appellant.

Still with respect to the independent claims, the Examiner has again relied on the Abstract; Col. 3, lines 54-67; and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "generating a report containing the identified network address and hosting authority" (see the same or similar, but not necessarily identical language in independent claims).

Appellant respectfully asserts that the only suggestion of a "report" in the excerpts relied on by the Examiner merely relates to "seed addresses [which] can alert an e-mail provider to potential mass mailings by reporting when mail is received for ghost or non-existent accounts." Clearly, alerting an e-mail provider when an e-mail is received for a seed address, as in Leeds, fails to even suggest "generating a report containing the identified network address and hosting authority" (emphasis added), as claimed by appellant.

Further, the Examiner argued that "Leeds also describes the similar process of identifying the host name of the spammer's address (please see col.4, lines 60-67 & col.5, lines 1-45)." Appellant disagrees and respectfully asserts that Leeds simply discloses that '[t]he fields for "Return Path:," "From:," and "Reply-To:" are highlighted as three of the fields which the present invention will parse from the message header.' As an example, Leeds teaches that "From: 48941493@notarealaddress.com is broken down into a user id (48941493) and a host name

(notarealaddress.com)" (emphasis added). Leeds continues, disclosing that 'a first level check is [used] to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid.'

Moreover, Leeds discloses that the first level check 'includ[es]: (1) sending a message to the user identified by the "From:" or "Reply-To:" fields and examining whether the message can be successfully delivered, (2) using the UNIX "whois" command to determine if a site (or host) by that name actually exists, (3) using the UNIX "finger" command to identify if a user name exists at a verifiable host, (4) using the "vrfy" command when connected to a sendmail daemon to verify that a user exists at a particular site, and (5) using the UNIX "traceroute" command to make sure there is a valid route back to the specified host' (emphasis added). Clearly, performing a first level check including using whois, and traceroute to verify the host name from the "From:" and "Reply-To:" fields, as in Leeds, fails to even suggest "generating a report containing the identified **network** address and hosting authority" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner asserts that "in addition to identifying the network address and hosting authority... Leeds discloses maintaining (1) a list of mail of certain mail providers (i.e. hosting authorities/ISPs) known to be an origination point of junk email... (2) a dictionary of certain content frequently found in junk email, and (3) a learning knowledge base that creates its own rules to ascertain prior junk e-mail characteristics" (emphasis removed), and that Leeds "subsequently adds those criteria to the knowledge base to prevent future junk e-mail with the same or similar characteristics from being delivered."

Further, the Examiner states that "Leeds discloses that the rules are continuously modified and maintained i.e. stored with the list of names and addresses of the spammers and their hosting authorities as new SPAM e-mails arrive," and that therefore "the list containing the names and addresses of the spammers and their hosting authorities can be called a report, which can be sent or transmitted to related authorities for appropriate action."

Appellant respectfully disagrees and notes that Leeds merely teaches "maintaining (1) a list of certain mail providers known to be an origination point of junk e-mail, (2) a dictionary of certain content frequently found in junk e-mail, and (3) a learning knowledge base that creates its own rules to ascertain prior junk e-mail characteristics" (Col. 4, lines 29-33 – emphasis added). However,

merely maintaining a list of mail providers as in Leeds, fails to specifically disclose "generating a report containing the identified network address and hosting authority" (emphasis added), as claimed by appellant.

Further, with respect to each of the independent claims, the Examiner has relied on Col. 4, lines 60-67; Col. 5, lines 1-44; and Col. 6, lines 52-65 in Leeds to make a prior art showing of appellant's claimed technique "wherein identifying the hosting authority comprises identifying an owner of a network domain" (see the same or similar, but not necessarily identical language in the independent claims).

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose 'a first level check is to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid' (emphasis added). In addition, Leeds discloses 'using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the "From:" or "Reply-To:" fields, as in Leeds, fails to even suggest a technique "wherein identifying the **hosting** authority comprises identifying an **owner** of a network domain" (emphasis added), as claimed by appellant. Appellant respectfully asserts that merely ensuring that a host actually exists fails to even suggest "identifying an owner of a network domain," as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner fails to respond to appellant's arguments with respect to appellant's claimed technique "wherein identifying the hosting authority comprises identifying an owner of a network domain." Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Appellant further notes that in the Examiner's Answer dated 07/02/2007, the Examiner argues that "appellant...alleges that there is not motivation to combine the prior art references," and that "Leeds... has a learning knowledge base that continually maintains a list of hosting authorities and addresses that are culprits of sending junk mail."

Appellant respectfully disagrees and notes that Leeds merely discloses maintaining a list of mail providers, a dictionary of common junk mail content, and a knowledge base which creates rules for determining junk mail characteristics, as mentioned above, which clearly does not specifically suggest a "learning knowledge base that continually maintains a list of...addresses that are culprits of sending junk mail" (emphasis added), as noted by the Examiner.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claims 2, 18, and 24

With respect to Claim 2 et al., the Examiner has relied on Col. 4, lines 36-67; Col. 5, lines 1-44; and Col. 8, lines 34-57 in Leeds to make a prior art showing of appellant's claimed "transmitting the generated report to the identified hosting authority."

Appellant respectfully asserts that the only mention of any sort of report, in such excerpts from Leeds, is the teaching that 'addresses could be watched for incoming junk e-mail and a notification from the authentication server could then be broadcast to users indicating that mail with the subject of "XYZ" is junk e-mail' (see, specifically, Col. 8, lines 47-50). Clearly, such notification sent to users does not meet appellant's claimed "transmitting the generated report to the identified hosting authority" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner alleges that "the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action." Further, the Examiner relies on Col. 3, lines 57-67 and Col. 4, lines 65-67 of Leeds and further states that "[t]he sender's origination information {I.E. sender's address: Spammer@aol.com} is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent," such that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM."

Appellant respectfully disagrees and again notes that merely maintaining a list of mail providers, as in Leeds, fails to specifically disclose a "list containing the names and addresses of the spammers and their hosting authorities" (emphasis added), as noted by the Examiner. Further, appellant notes that, in Leeds, the list of mail providers is used in "a determination of the status of mail as junk e-mail or a valid message" (Col. 4, lines 27-28 – emphasis added), and is not used to act as a report to be "transmitt[ed]... to the identified hosting authority" (emphasis added), as claimed by appellant.

Additionally, appellant respectfully points out that, as admitted by the Examiner, Col. 3, lines 57-67 of Leeds teaches that the "senders' origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent," such that a "verification response...is received in response to the verification request, [and] the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail" (Col. 3, lines 60-65 – emphasis added). However, extracting a sender's origination information from an e-mail message for sending a verification request, as in Leeds, does not even *suggest* "transmitting the generated report to the identified hosting authority" (emphasis added), as claimed by appellant. Appellant respectfully asserts that the excerpts from Leeds relied on by the Examiner simply do not suggest "transmitting the generated report to the identified hosting authority" (emphasis added), as claimed by appellant.

In view of the Examiner's argument that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority

administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM," it seems the Examiner has simply dismissed the same under Official Notice (since no specific prior art showing was made). In response, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Leeds. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP below.

"If the applicant traverses such an [Official Notice] assertion the examiner should cite a reference in support of his or her position." See MPEP 2144.03.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #3: Claim 4

With respect to Claim 4, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed technique "wherein identifying a URL comprises comparing text within the electronic message to a database of words to identify the URL."

After careful review of the excerpts relied on by the Examiner, appellant notes that the only URL disclosed in Aronson relates to filtering e-mail based on "feature extraction & analysis (e.g.,...URL's...)" (see Col. 5, lines 63-64). However, Aronson does not teach how such URL is identified, whereas appellant specifically claims "identifying a URL [by] comparing text within the electronic message to a database of words to identify the URL," as claimed. Appellant further notes that Aronson only teaches that spam may be filtered "based on a specific keyword search," and that therefore the keywords are used to identify spam, but not that a database of words is utilized to "identify the URL" (emphasis added), in the manner claimed by appellant.

In the Examiner's Answer dated 07/02/2007, it seems the Examiner has failed to specifically respond to appellant's above arguments. Specifically, the Examiner has only generally argued that

Aronson discloses "filter[ing] e-mail based on…feature extraction & analysis (e.g. based on…URL's…)."

However, merely disclosing filtering e-mail based on URLs, as in Aronson, does not teach a technique for "identifying a URL," and particularly not where "identifying a URL comprises comparing text within the electronic message to a database of words to identify the URL" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #4: Claim 5 and 6

With respect to Claim 5, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "comparing the identified URL to a database of legitimate URLs."

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added). Further, Aronson discloses that "[r]ules 210 based on keywords in the subject or body of spam e-mail may also be established" and '[f]or example, all e-mails containing the two words "sex" and "free" may be identified as spam and filtered' (Col. 4, lines 2-5 – emphasis added). In addition, Aronson discloses that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)" (Col. 5, lines 58-64 – emphasis added).

However, appellant respectfully asserts that Aronson's disclosure of filtering e-mail as spam based on keywords, the source address being identified as a known spammer, IP source frequency

analysis, and feature extraction and analysis, simply fails to even suggest "comparing the identified URL to a database of legitimate URLs" (emphasis added), as claimed by appellant. Clearly, filtering based on a feature extraction and analysis of a URL fails to suggest "comparing the identified URL to a database of legitimate URLs" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner states that 'Aronson on col.1, lines 52-55 discloses a well know[n] technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses).' In addition, the Examiner asserts that "col.5... line[s] 50-67 disclos[e] employing rule handling filter modules... to control SPAM," and that "RS(c) may be an inclusion list" (emphasis removed). The Examiner further notes that "all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network" (emphasis removed).

Appellant respectfully disagrees and points out that Aronson merely discloses that some "known e-mail filtering techniques are based upon an inclusion list, such that e-mail received from any source other than one listed in the inclusion list is discarded as junk" (Col.1, lines 52-55 – emphasis added). Additionally, Aronson teaches that a filter module "may be an inclusion list," and that "[o]ther... filter modules will filter e-mail based on... URL's," (Col. 5, lines 57-67 – emphasis added).

However, merely disclosing a filtering technique utilizing a e-mail source inclusion list, in addition to a general filtering technique based on URLs, does not specifically disclose "comparing the identified URL to a database of legitimate URLs" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #5: Claim 10

With respect to Claim 10, the Examiner has relied on Col. 3, lines 54-67; Col. 4, lines 1-23; Col. 4, lines 1-23 and 60-67; and Col. 5, lines 1-44; in Leeds to make a prior art showing of appellant's claimed technique "wherein identifying the hosting authority comprises identifying an Internet service provider."

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose that 'a first level check is to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid' (emphasis added). In addition, Leeds discloses 'using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the "From:" or "Reply-To:" fields, as in Leeds, fails to even suggest a technique "wherein identifying the hosting authority comprises identifying an Internet service provider" (emphasis added), as claimed by appellant. Appellant respectfully asserts that merely ensuring that a host actually exists fails to specifically suggest "identifying an Internet service provider," in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner asserts that 'it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. email address) can in fact be the Internet service provider (ISP),' and that "it is not possible to send e-mail or electronic mail without the presence of an Internet Service Provider." The Examiner goes on to argue that in 'a SPAM mail coming from, Spammer@aol.com... "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.'

In addition, the Examiner states that "Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent mails is SPAM mail or not." The Examiner then relies on Col. 3, lines 57-67 and Col. 4, lines 65-67 from Leeds and asserts that "Leeds further elaborates [on] the analysis process on Col. 4, lines 65-67."

Appellant respectfully disagrees and notes that the above reference excerpts relied on by the Examiner merely teach that "[t]he sender's origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent" (Col. 3, lines 59-61 – emphasis added). In addition, the excerpts teach that 48941493@notarealaddress.com is broken down into a user id (48941493) and a host name (notarealaddress.com) (Col. 4, lines 65-67 – emphasis added). Further still, appellant points out that, in Leeds, '[s]ince junk e-mails often come

from either non-existent users or non-existent sites or both, a first level check is to determine if the alleged sender[s] identified by the "From:" or "Reply-To:" fields are valid' and that '[t]his first level check corresponds to issuing a verification request and can be in many forms, including… using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (Col. 5, lines 16-25 – emphasis added).

However, merely extracting sender origination information, such as a host name, from an e-mail message header, and using a UNIX "whois" command to determine if the host actually exists, does not specifically teach a technique "wherein identifying the hosting authority comprises identifying an Internet service provider" (emphasis added), as claimed by appellant. Again, merely ensuring that a host actually exists fails to specifically suggest "identifying an Internet service provider," in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #6: Claim 11

With respect to Claim 11, the Examiner has relied on Col. 4, lines 36-67; Col. 5, lines 1-44; and Col. 8, lines 34-57 in Leeds to make a prior art showing of appellant's claimed "transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority."

Appellant respectfully asserts that the only mention of any sort of report in such excerpts from Leeds simply teaches that 'addresses could be watched for incoming junk e-mail and a notification from the authentication server could then be broadcast to users indicating that mail with the subject of "XYZ" is junk e-mail' (see, specifically, Col. 8, lines 47-50). However, such notification sent to users does not meet appellant's claimed "transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority" (emphasis added), as claimed by appellant. Clearly, sending a notification to users, as in Leeds, fails to meet "transmitting the report to a central managed service provider" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner argues that "the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action." Further, the Examiner relies on Col. 3, lines 57-67 and Col. 4, lines 65-67 of Leeds and further states that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in [a] similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM."

Appellant respectfully disagrees and again notes that merely maintaining a list of mail providers, as in Leeds, fails to specifically disclose a "list containing the names and addresses of the spammers and their hosting authorities" (emphasis added), as noted by the Examiner. Further, appellant notes that, in Leeds, the list of mail providers is used in "a determination of the status of mail as junk e-mail or a valid message" (Col. 4, lines 27-28 – emphasis added), and is not used to act as a report to be "transmitt[ed]… to a central managed service provider configured to forward the report to the identified hosting authority" (emphasis added), as specifically claimed by appellant.

Additionally, appellant respectfully points out that, as admitted by the Examiner, Col. 3, lines 57-67 of Leeds teaches that the "senders' origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent," such that a "verification response…is received in response to the verification request, [and] the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail" (Col. 3, lines 60-65 – emphasis added). However, extracting a sender's origination information from an e-mail message for sending a verification request, as in Leeds, does not even *suggest* "transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority" (emphasis added), as claimed by appellant. Appellant respectfully asserts that the excerpts from Leeds relied on by the Examiner simply do not suggest "transmitting the report to a central managed service provider configured to forward the report to the identified hosting authority" (emphasis added), as specifically claimed by appellant.

In view of the Examiner's argument that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM," it seems the Examiner has simply dismissed the same under Official Notice (since no specific prior art showing was made). In response, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Leeds. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP cited above.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #7: Claim 12

With respect to Claim 12, the Examiner has relied on Col. 5, lines 38-44 in Leeds to make a prior art showing of appellant's claimed technique including "at least temporarily saving the report and transmitting the report to the identified hosting authority at the end of a specified period."

Appellant respectfully asserts that such excerpt only relates to "sending a verification message…within a period of time." Clearly, sending a verification message to determine if a user is actually associated with the sender of e-mail does not meet appellant's claimed report, let alone "transmitting the report to the identified hosting authority at the end of a specified period" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner alleges that "the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action." Further, the Examiner relies on Col. 3, lines 57-67 and Col. 4, lines 65-67 of Leeds and further states that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in [a] similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an

attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM."

Appellant respectfully disagrees and again notes that merely maintaining a list of mail providers, as in Leeds, fails to specifically disclose a "list containing the names and addresses of the spammers and their hosting authorities" (emphasis added), as noted by the Examiner. Further, appellant notes that, in Leeds, the list of mail providers is used in "a determination of the status of mail as junk e-mail or a valid message" (Col. 4, lines 27-28 – emphasis added), and is not used to act as a report to be "transmitt[ed]... to the identified hosting authority at the end of a specified period" (emphasis added), as claimed by appellant.

Additionally, appellant respectfully points out that, as admitted by the Examiner, Col. 3, lines 57-67 of Leeds teaches that the "senders' origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent," such that a "verification response...is received in response to the verification request, [and] the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail" (Col. 3, lines 60-65 – emphasis added). However, extracting a sender's origination information from an e-mail message for sending a verification request, as in Leeds, does not even *suggest* "transmitting the report to the identified hosting authority at the end of a specified period" (emphasis added), as claimed by appellant.

In view of the Examiner's argument that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM," it seems the Examiner has simply dismissed the same under Official Notice (since no specific prior art showing was made). In response, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Leeds. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP cited above.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #8: Claim 16

With respect to Claim 16, the Examiner has relied on Col. 3, lines 54-67; Col. 4, lines 1-23 and 60-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant's claimed technique "wherein the hosting authority is an Internet service provider."

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose that 'a first level check is to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid' (emphasis added). In addition, Leeds discloses 'using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the "From:" or "Reply-To:" fields, as in Leeds, fails to even suggest a technique "wherein the hosting authority is an Internet service provider" (emphasis added), as claimed by appellant. Appellant respectfully asserts that merely ensuring that a host actually exists fails to specifically suggest a "hosting authority [that] is an Internet service provider," as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner asserts that 'it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. email address) can in fact be the Internet service provider (ISP)' and that "it is not possible to send e-mail or electronic mail without the presence of an Internet Service Provider." The Examiner goes on to argue that in 'a SPAM mail coming from, Spammer@aol.com... "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.'

In addition, the Examiner states that "Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent mails is SPAM mail or not." The Examiner then relies on Col. 3, lines 57-67; Col. 4, lines 65-67; and Col. 5, lines 13-33 from Leeds and asserts that "Leeds clearly discloses identifying the hosting authority that is hosting the network address."

Appellant respectfully disagrees and notes that the above reference excerpts relied on by the Examiner merely teach that "[t]he sender's origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent" (Col. 3, lines 59-61 – emphasis added). In addition, the excerpts teach that 48941493@notarealaddress.com is broken down into a user id (48941493) and a host name (notarealaddress.com) (Col. 4, lines 65-67 – emphasis added). Further still, the excerpts teach that '[s]ince junk e-mails often come from either non-existent users or non-existent sites or both, a first level check is to determine if the alleged sender[s] identified by the "From:" or "Reply-To:" fields are valid' and that '[t]his first level check corresponds to issuing a verification request and can be in many forms, including… using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (Col. 5, lines 16-25 – emphasis added).

However, merely extracting sender origination information, such as a host name, from an e-mail message header, and using a UNIX "whois" command to determine if the host actually exists, does not specifically teach a technique "wherein the hosting authority is an Internet service provider" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #9: Claim 19

With respect to Claim 19, the Examiner has relied on Col. 4, lines 36-67; Col. 5, lines 1-44; and Col. 8, lines 34-57 in Leeds to make a prior art showing of appellant's claimed technique "wherein the processor is configured to transmit the report to a central managed service provider."

Appellant respectfully asserts that the only mention of any sort of report in such excerpts from Leeds simply teaches that 'addresses could be watched for incoming junk e-mail and a notification from the authentication server could then be broadcast to users indicating that mail with the subject of "XYZ" is junk e-mail' (see, specifically, Col. 8, lines 47-50). However, such notification sent to users does not meet appellant's claimed "transmit[ting] the report to a central managed service

provider" (emphasis added), as claimed by appellant. Clearly, sending a notification to users, as in Leeds, fails to meet "transmit[ting] the report to a central managed service provider" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner alleges that "the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action." Further, the Examiner relies on Col. 3, lines 57-67 and Col. 4, lines 65-67 of Leeds and further states that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in [a] similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM."

Appellant respectfully disagrees and again notes that merely maintaining a list of mail providers, as in Leeds, fails to specifically disclose a "list containing the names and addresses of the spammers and their hosting authorities" (emphasis added), as noted by the Examiner. Further, appellant notes that, in Leeds, the list of mail providers is used in "a determination of the status of mail as junk e-mail or a valid message" (Col. 4, lines 27-28 – emphasis added), and is not used to act as a report to be "transmitt[ed]... to a central managed service provider" (emphasis added), as claimed by appellant.

Additionally, appellant respectfully points out that, as admitted by the Examiner, Col. 3, lines 57-67 of Leeds teaches that the "senders' origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent," such that a "verification response...is received in response to the verification request, [and] the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail" (Col. 3, lines 60-65 – emphasis added). However, extracting a sender's origination information from an e-mail message for sending a verification request, as in Leeds, does not even *suggest* a technique "wherein the processor is configured to transmit the report to a central managed service provider" (emphasis added), as claimed by appellant.

In view of the Examiner's argument that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM," it seems the Examiner has simply dismissed the same under Official Notice (since no specific prior art showing was made). In response, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Leeds. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP cited above.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #10: Claim 20

With respect to Claim 20, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "database containing search terms used to identify the network address within text of the electronic message."

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added). Further, Aronson discloses that "[r]ules 210 based on keywords in the subject or body of spam e-mail may also be established" and '[f]or example, all e-mails containing the two words "sex" and "free" may be identified as spam and filtered' (Col. 4, lines 2-5 – emphasis added). In addition, Aronson discloses that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)" (Col. 5, lines 58-64 – emphasis added).

However, Aronson's mere disclosure that the network address contained within the source header is used by a rule to filter e-mail from this network address to a spam storage area simply fails to even suggest that "a database containing search terms [is] used to identify the network address within text of the electronic message" (emphasis added), in the manner claimed by appellant. Further, disclosing identifying and filtering spam based on keywords in the subject or body, as in Aronson, fails to suggest that "a database containing search terms [is] used to identify the network address within text of the electronic message" (emphasis added), as claimed by appellant. In addition, Aronson's disclosure that rule handling filter modules will filter e-mail based on IP source frequency analysis, and feature extraction & analysis simply fails to suggest that "a database containing search terms [is] used to identify the network address within text of the electronic message" (emphasis added), as claimed by appellant. Clearly, identifying and filtering spam based on keywords and features, as in Aronson, fails to meet "a database containing search terms used to identify the network address" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner states that "Aronson on col.1, lines 52-55 discloses a well know[n] technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses)." In addition, the Examiner asserts that "col.5... line[s] 50-67 disclos[e] employing rule handling filter modules... to control SPAM" and that "RS(c) may be an inclusion list" (emphasis removed). The Examiner further notes that "all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network" (emphasis removed). Further still, the Examiner relies on Col. 6, lines 47-52 of Aronson as "further elaborat[ing on] one of the rules."

Appellant respectfully disagrees and points out that Aronson merely discloses that some "known e-mail filtering techniques are based upon an inclusion list, such that e-mail received from any source other than one listed in the inclusion list is discarded as junk" (Col.1, lines 52-55 – emphasis added). Additionally, Aronson teaches that a filter module "may be an inclusion list" and that "[o]ther... filter modules will filter e-mail based on... addresses," and also that "all of the rule handling filter modules described herein may be combined" (Col. 5, lines 57-67 – emphasis added). Furthermore, Aronson discloses that 'a rule which is geared towards screening e-mail messages containing sexual content... which filters e-mail based on the keywords "sex" and "free" may be given a weight value of 10 on a scale from 1 to 10' (Col. 6, lines 47-51 – emphasis added).

However, merely disclosing a filtering technique utilizing a e-mail source inclusion list, in addition to a general filtering technique based on addresses, does not teach "a database containing search terms used to identify the network address within text of the electronic message" (emphasis added), as claimed by appellant. More specifically, filtering e-mail based on keywords, as in Aronson, fails to meet "a database containing search terms used to identify the network address" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #11: Claim 21

With respect to Claim 21, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "database containing a list of trusted network addresses."

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added). However, appellant respectfully asserts that Aronson's disclosure of filtering e-mail as spam based on the source address being identified as a known spammer simply fails to even suggest "a database containing a list of **trusted** network addresses" (emphasis added), as claimed by appellant. Clearly, a source address of a known spammer, as in Aronson, simply fails to suggest "a list of **trusted** network addresses" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner states that "Aronson on col.1, lines 52-55 discloses a well know[n] technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses)." In addition, the Examiner asserts that "col.5... line[s] 50-67 disclos[e] employing rule handling filter modules... to control SPAM" and that "RS(c) may be an inclusion list" (emphasis removed). The Examiner further notes that "all of the rule

handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network" (emphasis removed).

Appellant respectfully disagrees and points out that Aronson merely discloses that some "known e-mail filtering techniques are based upon an inclusion list, such that e-mail received from any source other than one listed in the inclusion list is discarded as junk" (Col.1, lines 52-55 – emphasis added). Additionally, Aronson teaches that a filter module "may be an inclusion list," that "[o]ther… filter modules will filter e-mail based on… addresses," and also that "all of the rule handling filter modules described herein may be combined" (Col. 5, lines 57-67 – emphasis added).

However, merely disclosing a filtering technique utilizing a e-mail source inclusion list in addition to a general filtering technique based on addresses, does not teach "a database containing a list of trusted network addresses" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #12: Claims 22 and 23

With respect to independent Claim 22, the Examiner has relied on Col. 4, lines 51-56; Col. 5, lines 50-67; and the Abstract in Aronson along with Col. 3, lines 54-67; and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "code that identifies an authority hosting the network address."

Appellant respectfully asserts that the excerpts from Leeds relied on by the Examiner only relate to a host computer associated with a sender of an electronic mail message (see Abstract and Col. 4, lines 66-67, specifically). In addition, Leeds discloses that "if a message has purportedly been relayed through a machine named mail.frommowhere.com and the mail handling system has determined that such a machine does not actually exist, the confidence rating for the message should be increased." Clearly, determining a host computer/host name of a sender of e-mail or relay, as in Leeds, does not meet appellant's specific claim language, namely an "authority hosting the **network** address" (emphasis added), as claimed by appellant.

Further, appellant respectfully asserts that the excerpts from Aronson relied upon by the Examiner merely disclose that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1) word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)" (emphasis added). Clearly, filtering e-mail based on IP source frequency and feature extraction & analysis fails to even suggest "identify[ying] an authority hosting the **network** address" (emphasis added), as claimed by appellant.

In addition, the Examiner argued that "Ar[o]nson disclosed that the source header data from an incoming e-mail address (aardvark@aol.com) is analyzed by the spam probes." Further, the Examiner argued that '[t]he source header data includes the ISP (in this case "aol") hosting the spammer's network address (see col.4, lines 45-67).' Appellant disagrees and respectfully asserts that the excerpt from Aronson simply discloses that "[a] spam probe is an e-mail address selected to make its way onto as many spam mailing lists as possible." Aronson continues, teaching that "[i]t is also selected to appear high up on spammers' lists in order to receive spam mailings early in the mailing process" using an e-mail address such as "aardvark@aol.com." Clearly, the mere disclosure of using an e-mail address in a spam probe, as in Aronson, completely fails to even suggest "identify[ying] an authority hosting the **network** address" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner asserts that 'it is evident that a "hosting authority" or a "authority hosting" the network address (i.e. email address) can in fact be the Internet service provider (ISP)' and that "it is not possible to send e-mail or electronic mail without the presence of an Internet Service Provider." The Examiner goes on to allege that in 'a SPAM mail coming from, Spammer@aol.com... "aol.com" signifies the identity of the hosting authority that supports/hosts (i.e. maintains information in its servers that uniquely identifies the Spammer) the Spammer's address.'

In addition, the Examiner states that "Leeds in particular discloses a method of reducing junk mail (SPAM) in which various filters are applied to the incoming mail to determine whether the sent

mails is SPAM mail or not." The Examiner then relies on Col. 3, lines 57-67; Col. 4, lines 65-67; and Col. 5, lines 13-33 from Leeds and asserts that "Leeds clearly discloses identifying the hosting authority that is hosting the network address."

Appellant respectfully disagrees and notes that the above reference excerpts relied on by the Examiner merely teach that "[t]he sender's origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent" (Col. 3, lines 59-61 – emphasis added). In addition, the excerpts teach that 48941493@notarealaddress.com is broken down into a user id (48941493) and a host name (notarealaddress.com) (Col. 4, lines 65-67 – emphasis added). Further still, the excerpts teach that '[s]ince junk e-mails often come from either non-existent users or non-existent sites or both, a first level check is to determine if the alleged senderfs] identified by the "From:" or "Reply-To:" fields are valid' and that '[t]his first level check corresponds to issuing a verification request and can be in many forms, including... using the UNIX "whois" command to determine if a site (or host) by that name actually exists' (Col. 5, lines 16-25 – emphasis added).

However, merely extracting sender origination information, such as a host name, from an e-mail message header, and using a UNIX "whois" command to determine if the host actually exists, as in Leeds, does not teach "code that identifies an authority hosting the **network** address" (emphasis added), as claimed by appellant.

Still with respect to independent Claim 22, the Examiner has again relied on the Abstract; Col. 3, lines 54-67; and Col. 4, lines 1-35 in Leeds to make a prior art showing of appellant's claimed "code that generates a report containing the identified network address."

Appellant respectfully asserts that the only suggestion of a "report" in the excerpts relied on by the Examiner merely relates to "seed addresses [which] can alert an e-mail provider to potential mass mailings by reporting when mail is received for ghost or non-existent accounts." Clearly, alerting an e-mail provider when an e-mail is received for a seed address, as in Leeds, fails to even suggest "generat[ing] a report containing the identified network address" (emphasis added), as claimed by appellant.

Further, the Examiner argued that "Leeds also describes the similar process of identifying the host name of the spammer's address (please see col.4, lines 60-67 & col.5, lines 1-45)." Appellant disagrees and respectfully asserts that Leeds simply discloses that '[t]he fields for "Return Path:," "From:," and "Reply-To:" are highlighted as three of the fields which the present invention will parse from the message header.' As an example, Leeds teaches that "From: 48941493@notarealaddress.com is broken down into a user id (48941493) and a host name (notarealaddress.com)" (emphasis added). Leeds continues, disclosing that 'a first level check is [used] to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid.' Moreover, Leeds discloses that the first level check 'includ[es]: (1) sending a message to the user identified by the "From:" or "Reply-To:" fields and examining whether the message can be successfully delivered, (2) using the UNIX "whois" command to determine if a site (or host) by that name actually exists, (3) using the UNIX "finger" command to identify if a user name exists at a verifiable host, (4) using the "vrfy" command when connected to a sendmail daemon to verify that a user exists at a particular site, and (5) using the UNIX "traceroute" command to make sure there is a valid route back to the specified host' (emphasis added). Clearly, performing a first level check including using whois, and traceroute to verify the host name from the "From:" and "Reply-To:" fields, as in Leeds, fails to even suggest "generat[ing] a report containing the identified **network** address" (emphasis added), as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner failed to respond to appellant's arguments with respect to appellant's claimed "code that generates a report containing the identified network address." Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Further, with respect to independent Claim 22, the Examiner has relied on Col. 4, lines 60-67; Col. 5, lines 1-44; and Col. 6, lines 52-65 in Leeds to make a prior art showing of appellant's claimed technique "wherein identifying the hosting authority comprises identifying an owner of a network domain."

Appellant respectfully asserts that the excerpts from Leeds relied upon by the Examiner merely disclose 'a first level check is to determine if the alleged sender identified by the "From:" or "Reply-To:" fields are valid' (emphasis added). In addition, Leeds discloses 'using the UNIX "whois"

command to determine if a site (or host) by that name actually exists' (emphasis added). Clearly, using whois to perform a first level check to ensure the host actually exists for the alleged sender in the "From:" or "Reply-To:" fields, as in Leeds, fails to even suggest a technique "wherein identifying the **hosting** authority comprises identifying an **owner** of a network domain" (emphasis added), as claimed by appellant. Appellant respectfully asserts that merely ensuring that a host actually exists fails to even suggest "identifying an owner of a network domain," as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner failed to respond to appellant's arguments with respect to appellant's claimed technique "wherein identifying the hosting authority comprises identifying an owner of a network domain." Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #13: Claim 25

With respect to Claim 25, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "code that compares text within the electronic message to a database of words to locate the network address within the text."

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added). Further, Aronson discloses that "[r]ules 210 based on keywords in the subject or body of spam e-mail may also be established" and '[f]or example, all e-mails containing the two words "sex" and "free" may be identified as spam and filtered' (Col. 4, lines 2-5 – emphasis added). In addition, Aronson discloses that "[o]ther contemplated rule handling filter modules will filter e-mail based on: (1)

word or letter frequency analysis; (2) IP source frequency analysis; (3) misspelling analysis (unwanted e-mail often contains misspelled words); (4) word or letter combination analysis; (5) technical or legal RFC822 header compliance; and (6) feature extraction & analysis (e.g., based on phone numbers, URL's, addresses, etc.)" (Col. 5, lines 58-64 – emphasis added).

However, the mere disclosure that the network address contained within the source header is used by a rule to filter e-mail from this network address to a spam storage area, as in Aronson, simply fails to even suggest "code that compares text within the electronic message to a database of words to locate the network address within the text" (emphasis added), in the manner claimed by appellant. Further, Aronson's disclosure to identify and filter spam based on keywords in the subject or body fails to suggest "code that compares text within the electronic message to a database of words to locate the network address within the text" (emphasis added), as claimed by appellant. In addition, Aronson's disclosure that rule handling filter modules will filter e-mail based on IP source frequency analysis, and feature extraction & analysis simply fails to suggest "code that compares text within the electronic message to a database of words to locate the network address within the text" (emphasis added), as claimed by appellant. Clearly, identifying and filtering spam based on keywords and features, as in Aronson, fails to meet "a database of words to locate the network address within the text" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner states that "Aronson on col.1, lines 52-55 discloses a well know[n] technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses)." In addition, the Examiner asserts that "col.5… line[s] 50-67 disclos[e] employing rule handling filter modules… to control SPAM" and that "RS(c) may be an inclusion list" (emphasis removed). The Examiner further notes that "all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network" (emphasis removed).

Appellant respectfully disagrees and points out that Aronson merely discloses that some "known e-mail filtering techniques are based upon an inclusion list, such that e-mail received from any source other than one listed in the inclusion list is discarded as junk" (Col.1, lines 52-55 – emphasis added). Additionally, Aronson teaches that a filter module "may be an inclusion list" and that "[o]ther…

filter modules will filter e-mail based on... addresses," and also that "all of the rule handling filter modules described herein may be combined" (Col. 5, lines 57-67 – emphasis added).

However, merely disclosing a filtering technique utilizing a e-mail source inclusion list in addition to a general filtering technique based on addresses, does not teach a technique "to locate the network address within the text," as claimed, let alone specifically that "code...compares text within the electronic message to a database of words to locate the network address within the text" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #14: Claim 26

With respect to Claim 26, the Examiner has relied on Col. 4, lines 57-67; Col. 5, lines 1-8; and Col. 5, lines 50-67 in Aronson to make a prior art showing of appellant's claimed "code that compares the identified network address with trusted network addresses."

After careful review of the excerpts relied on by the Examiner, appellant notes that Aronson merely discloses that "[i]f the network address contained in the source header is identified as the network address of a known spammer, a rule will be established to filter all incoming e-mail from this network address into the spam storage area 230" (Col. 4, lines 60-62 – emphasis added).

However, appellant respectfully asserts that Aronson's disclosure of filtering e-mail as spam based on the source address being identified as a known spammer simply fails to even suggest "code that compares the identified network address with trusted network addresses" (emphasis added), as claimed by appellant. Clearly, the source address of a known spammer, as in Aronson, simply fails to suggest "trusted network addresses" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner states that "Aronson on col.1, lines 52-55 discloses a well know[n] technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses)." In addition, the Examiner asserts that "col.5...

line[s] 50-67 disclos[e] employing rule handling filter modules… to control SPAM" and that "RS(c) may be an inclusion list" (emphasis removed). The Examiner further notes that "all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network" (emphasis removed).

Appellant respectfully disagrees and points out that Aronson merely discloses that some "known e-mail filtering techniques are based upon an inclusion list, such that e-mail received from any source other than one listed in the inclusion list is discarded as junk" (Col.1, lines 52-55 – emphasis added). Additionally, Aronson teaches that a filter module "may be an inclusion list" and that "[o]ther… filter modules will filter e-mail based on… addresses," and also that "all of the rule handling filter modules described herein may be combined" (Col. 5, lines 57-67 – emphasis added).

However, merely disclosing a filtering technique utilizing a e-mail source inclusion list in addition to a general filtering technique based on addresses, does not teach "code that compares the identified network address with trusted network addresses" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #15: Claim 29

With respect to Claim 29, the Examiner has relied on Col. 4, lines 37-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant's claimed technique "wherein the report is utilized to generate an electronic mail message to be sent to the identified organization."

Appellant respectfully asserts that Leeds merely discloses "automatically sending a reply (in the form of a verification request) to the purported sender(s)" (Col. 4, lines 38-40 – emphasis added). Further, Leeds discloses 'issuing a verification request and can be in many forms, including: (1) sending a message to the user identified by the "From:" or "Reply-To:" fields and examining whether the message can be successfully delivered' (Col. 5, lines 20-23 – emphasis added). However, such verification request message sent to users fails to meet a technique "wherein the report is utilized to generate an electronic mail message to be sent to the identified organization"

(emphasis added), as claimed by appellant. Clearly, sending a verification message to the purported senders, as in Leeds, fails to meet "an electronic mail message to be sent to the identified organization" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner alleges that "the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action." Further, the Examiner relies on Col. 3, lines 57-67 and Col. 4, lines 65-67 of Leeds and further states that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in [a] similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM."

Appellant respectfully disagrees and again notes that merely maintaining a list of mail providers, as in Leeds, fails to specifically disclose a "list containing the names and addresses of the spammers and their hosting authorities" (emphasis added), as noted by the Examiner. Further, appellant notes that, in Leeds, the list of mail providers is used in "a determination of the status of mail as junk e-mail or a valid message" (Col. 4, lines 27-28 – emphasis added), and is not used to act as a report "utilized to generate an electronic mail message to be sent to the identified organization" (emphasis added), as claimed by appellant.

Additionally, appellant respectfully points out that, as admitted by the Examiner, Col. 3, lines 57-67 of Leeds teaches that the "senders' origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent," such that a "verification response…is received in response to the verification request, [and] the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail" (Col. 3, lines 60-65 – emphasis added). However, extracting a sender's origination information from an e-mail message for sending a verification request, as in Leeds, does not even *suggest* a technique "wherein the report is utilized to generate an electronic mail message to be sent to the identified organization" (emphasis added), as claimed by appellant.

In view of the Examiner's argument that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM," it seems the Examiner has simply dismissed the same under Official Notice (since no specific prior art showing was made). In response, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Leeds. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP cited above.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #16: Claim 30

With respect to Claim 30, the Examiner has relied on Col. 4, lines 36-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant's claimed technique "wherein identifying the URL further comprises examining text surrounding the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages."

Appellant respectfully asserts that Leeds merely discloses that "previously read junk e-mail can be added to the rules base to look for certain phrases" and that "[t]his may not be sufficient, however, to screen out valid mail that cites or quotes from the junk e-mail." (Col. 4, lines 52-56 – emphasis added). Further, Leeds discloses that "[i]f, however, the content is combined with an address that cannot pass a verification request, the user may wish to assign a 100% confidence rating, and the mail can optionally be automatically deleted" (Col. 4, lines 56-59). However, the mere disclosure of looking for certain phrases, as in Leeds, simply fails to even suggest a technique "wherein identifying the URL further comprises examining text **surrounding** the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages" (emphasis added), as claimed by appellant. Clearly, looking for certain phrases fails to specifically suggest "examining text surrounding the URL" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner states that "Aronson on col.1, lines 52-55 discloses a well know[n] technique of filtering the e-mail by comparing it with the "inclusion list" (i.e. list or database of trusted addresses)." In addition, the Examiner asserts that "col.5... line[s] 50-67 disclos[e] employing rule handling filter modules... to control SPAM" and that "RS(c) may be an inclusion list" (emphasis removed). The Examiner further notes that "all of the rule handling filter modules described herein may be combined or applied over a distributed array of filters throughout a network" (emphasis removed).

Appellant respectfully disagrees and points out that Aronson merely discloses that some "known e-mail filtering techniques are based upon an inclusion list, such that e-mail received from any source other than one listed in the inclusion list is discarded as junk" (Col.1, lines 52-55 – emphasis added). Additionally, Aronson teaches that a filter module "may be an inclusion list" and that "[o]ther... filter modules will filter e-mail based on... word or letter combination analysis," and also that "all of the rule handling filter modules described herein may be combined" (Col. 5, lines 57-67 – emphasis added).

However, merely disclosing a filtering technique utilizing a e-mail source inclusion list in addition to a general filtering technique based on word or letter combination analysis, in addition to disclosing that modules may be combined, does not teach "examining text surrounding the URL to determine a likelihood that the URL is an address of a web site associated with unsolicited messages" (emphasis added), as claimed by appellant. More specifically, general word or letter combination analysis fails to specifically disclose "determin[ing] a likelihood that the URL is an address of a web site associated with unsolicited messages" (emphasis added), in the manner as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

Group #17: Claim 31

With respect to Claim 31, the Examiner has relied on Col. 4, lines 36-67; and Col. 5, lines 1-44 in Leeds to make a prior art showing of appellant's claimed technique "wherein the report includes disclaimer information and user definable text."

Appellant respectfully asserts that Leeds merely discloses "automatically sending a reply (in the form of a verification request) to the purported sender(s)" (Col. 4, lines 38-40 – emphasis added). Further, Leeds discloses 'issuing a verification request and can be in many forms, including: (1) sending a message to the user identified by the "From:" or "Reply-To:" fields and examining whether the message can be successfully delivered' (Col. 5, lines 20-23 – emphasis added). However, such verification request message sent to users, as in Leeds, fails to even suggest a technique "wherein the report includes disclaimer information and user definable text" (emphasis added), as claimed by appellant. Clearly, the mere disclosure of a verification request fails to suggest "disclaimer information and user definable text" (emphasis added), in the manner as claimed by appellant.

In the Examiner's Answer dated 07/02/2007, the Examiner alleges that "the list containing the names and addresses of the spammers and their hosting authorities is technically a report, which can be sent or transmitted to related authorities for appropriate action." Further, the Examiner relies on Col. 3, lines 57-67 and Col. 4, lines 65-67 of Leeds and further states that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in [a] similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing a disclaimer information and user definable text (i.e. network address uniquely identifying the user)."

Appellant respectfully disagrees and again notes that merely maintaining a list of mail providers, as in Leeds, fails to specifically disclose a "list containing the names and addresses of the spammers and their hosting authorities" (emphasis added), as noted by the Examiner. Further, appellant notes that, in Leeds, the list of mail providers is used in "a determination of the status of mail as junk e-mail or a valid message" (Col. 4, lines 27-28 – emphasis added), and is not used to act as a "report includ[ing] disclaimer information and user definable text" (emphasis added), as claimed by appellant.

Additionally, appellant respectfully points out that, as admitted by the Examiner, Col. 3, lines 57-67 of Leeds teaches that the "senders' origination information is extracted from the e-mail message and an automatic reply (called a verification request) is created and sent," such that a "verification response…is received in response to the verification request, [and] the sender is scored as to the probable characteristics, origination, validity, and desirability of the mail" (Col. 3, lines 60-65 – emphasis added). However, extracting a sender's origination information from an e-mail message for sending a verification request, as in Leeds, does not even *suggest* a technique "wherein the report includes disclaimer information and user definable text" (emphasis added), as claimed by appellant.

In view of the Examiner's argument that "[i]t would have been obvious to one [of] ordinary skill in the art to send an e-mail in the similar way to the administrator@aol.com or any hosting authority administering the hosting along with [a] list as an attachment [as] disclosed by Leeds containing hosting authority and its associated respective network addresses that originate SPAM," it seems the Examiner has simply dismissed the same under Official Notice (since no specific prior art showing was made). In response, appellant again points out the remarks above that clearly show the manner in which some of such claims further distinguish Leeds. Appellant thus formally requests a specific showing of the subject matter in ALL of the claims in any future action. Note excerpt from MPEP cited above.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, as noted above.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P314).

Respectfully submitted,

By: /KEVINZILKA/ Date: September 4, 2007
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660